National Crime Prevention and Privacy Compact

COMPACT COUNCIL MEETING
DENVER, COLORADO
NOVEMBER 3-4, 2004
MINUTES

Ms. Donna Uzzell, Chairman, National Crime Prevention and Privacy Compact Council (Council), called the Council meeting to order at 9:00 a.m. on November 3, 2004, in the Grand Ballroom of the Hyatt Regency Denver in Denver, Colorado.

Mr. Robert Armstrong, State Compact Officer from the Colorado Bureau of Investigation provided opening remarks and welcomed attendees to Denver.

Mr. Todd C. Commodore, FBI's Criminal Justice Information Services (CJIS) Division's Compact Officer, conducted roll call of the Council members. The following Council members, or their proxies, were in attendance.

State Compact Officers:

- Ms. Debbie McKinney, Oklahoma State Bureau of Investigation (Proxy for Mr. Rusty Featherstone)
- Mr. Paul Heppner, Georgia Bureau of Investigation
- Ms. Julie LeTourneau, Minnesota Bureau of Criminal Apprehension
- Captain Timothy McGrail, Missouri State Highway Patrol
- Lt. John O'Brien, New Jersey Division of State Police
- Mr. Wilbur Rehmann, Montana Department of Justice
- Mr. David Sim, Kansas Bureau of Investigation
- Lt. Laurence Burns, Arizona Department of Public Safety (Proxy for Mr. Michael Timmerman)
- Ms. Donna Uzzell, Florida Department of Law Enforcement

State/Local Noncriminal Justice Agency Representative:

- Mr. Robert Finlayson III, Georgia Department of Human Resources

State/Local Criminal Justice Agency Representative:

- Ms. Carole Shelton, Maryland Department of Public Safety and Correctional Services

Federal Noncriminal Justice Agency Representative:

- Ms. Lana Adams, Office of Personnel Management (Proxy for Ms. Kathy Dillaman)

Federal Criminal Justice Agency Representative:

- Mr. Jonathan Frenkel, Department of Homeland Security

CJIS Advisory Policy Board (APB) Representative:

- Mr. Frank Sleeter, Sun Prairie Police Department, Sun Prairie, Wisconsin

Federal Bureau of Investigation:

- Mr. Jerome Pender, FBI, CJIS Division

Other meeting attendees introduced themselves and the agency they represented. **(Attachment 1)**

In recognition of Mr. Wilbur Rehmann's contribution to the Council and his pending retirement from the Montana Department of Justice, Mr. Jerome Pender, FBI's CJIS Division, presented a letter and certificate from the FBI thanking Mr. Rehmann for his years of service with the Council. Mr. Paul Heppner, on behalf of the CJIS Advisory Policy Board (APB), commended Mr. Rehmann's efforts and skills in coordinating delicate issues involving the CJIS APB and the Council. Chairman Donna Uzzell presented Mr. Rehmann with a letter on behalf of the Council acknowledging his contributions to the Council and his service as the Council's first Chairman. Chairman Uzzell commended Mr. Rehmann's leadership abilities and how his experience guided the Council during its formative stages and throughout his tenure as Chairman. During that time, twenty-one states ratified the Compact and twelve states executed the Council's Memorandum of Understanding (MOU).

Next, the Council approved the minutes from the May 2004 meeting.

Compact Council Action: **Mr. David Sim made a motion to approve the May 2004 minutes. The motion was approved by acclamation.**

Due to the vacancy of the Council's Vice-Chairman position, Chairman Uzzell conducted a special election to fill the vacant Council's Vice-Chairman position. She reviewed applicable Sections 7.2, 7.3, and 7.4 of the Bylaws regarding elections and opened the floor for nominations. Mr. Paul Heppner nominated Mr. David Sim. Captain Tim McGrail seconded the nomination. No other nominations were made for Vice-Chairman.

Compact Council Action: **Mr. Paul Heppner made a motion to close the nominations for Vice-Chairman. The motion was seconded by Captain Tim McGrail. Mr. Sim won the election by acclamation.**

Topic 1 **Standards Committee Report on the Establishment of Minimum Standards for Identification Verification of Applicants When Being Fingerprinted**

Mr. Scott Phillips, FBI's Council staff, presented information to the Council regarding FBI Council staff's efforts on establishing minimum standards for verifying the identity of applicants when being fingerprinted. **(Attachment 2)**

The FBI's Council staff examined different efforts in the development of biometric-based identification forms, the different models employed by states and agencies for verifying an applicants identity, and the chain of custody issue.

Chairman Uzzell requested the Council members forward their ideas regarding identification verification to her, the FBI's Council staff, or the Standards Committee. The Standards Committee will address this topic in more detail at its next meeting and provide recommendations to the Council for its consideration at the spring 2005 Council meeting.

Chairman Uzzell then announced that Mr. Paul Heppner would be the new chairman of the Standards Committee and thanked him for accepting the position.

Compact Council Action: **This topic was accepted as information only.**

Topic 2 **Standards Committee Report on the Outsourcing Proposed Rule and the Draft Security and Management Control Standards**

Mr. Wilbur Rehmann provided background information regarding the Outsourcing Proposed rule. He explained that at the request of the FBI in April 2002, the Council began examining methods and procedures to permit the outsourcing of noncriminal justice administrative functions involving access to criminal history record information (CHRI).
In May 2004, the Transportation Security Administration (TSA) solicited the Council to publish the Outsourcing rule to authorize their use of third party vendors for the Hazardous Materials (Hazmat) program. The Council agreed to prepare a limited scope rule on TSA's behalf before the November 2004 Council meeting. However, the FBI's Council staff, in consultation with Chairman Uzzell, decided not to proceed with the limited scope rule as the proposed rule was nearing completion. Therefore, the FBI's Council staff incorporated the comments from the
May 2004 Council meeting and submitted the Outsourcing rule and the standards to the Federal Register on October 28, 2004, to be published together. **(Attachments 3 and 4)**

Ms. Barbara Wiles, FBI's Council staff, described the significant changes to the Outsourcing rule since May 2004. The rule now includes only a reference to the CJIS security policy as the specific citations from the CJIS security policy were removed. The FBI's Office of the General Counsel (OGC), as well as the U.S. Department of Justice (DOJ) Office of Legal Policy, provided their comments. The Council's Executive Committee reviewed and approved the changes, Chairman Uzzell signed the rule, and the FBI's Council staff forwarded it to the Federal Register.

Following the day's meeting, the Council met out of session to discuss the status of the Outsourcing rule and how to accommodate TSA's prior request regarding an Interim Final Rule (IFR) and the fact that the CJIS Division had submitted the proposed rule to the Federal Register for publishing. Mr. Commodore reported that he had contacted the DOJ and requested that they hold the final rule in abeyance. To accommodate TSA's needs, the Council decided to publish the rule as an IFR to be effective on the date published (sometime before the end of the 2004 calendar year) so that the entities who need to use the Outsourcing rule may do so.

Compact Council Action: **Ms. Carole Shelton made a motion to accept the Outsourcing Proposed Rule and the Draft Security and Management Control Standards with the proposed changes, as an interim final rule with an effective date of December 31, 2004. Mr. Robert Finlayson seconded the motion. Motion carried.**

Topic 3 Update on TSA Hazmat Program

Mr. Commodore, FBI Compact Officer, explained that during the May 2004 Council meeting, the Council requested the FBI's Council staff to prepare a limited scope rule for TSA to accommodate their implementation of Section 1012 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). Following subsequent dialogue between the FBI's Council staff, the Council's Executive Committee, and the Council's Standards Committee, they decided to publish the Outsourcing rule, which was submitted to the Federal Register. Mr. Commodore further explained that TSA had met the three requirements from the motion that was made at the last Council meeting regarding outsourcing.

Next, Ms. Paula Barron, FBI's Council staff, updated the Council regarding TSA's Hazmat program. She briefed the Council about the American Association of Motor Vehicle Administrators (AAMVA) - USA PATRIOT Act working group. The working group consists of approximately twenty representatives from various state Department of Motor Vehicle (DMV) agencies. AAMVA and TSA work closely to conduct security threat assessments. Ms. Barron serves as the CJIS Division's liaison to the AAMVA - USA PATRIOT Act working group regarding the various initiatives involving the CJIS Division and the Council.

Next, Mr. Rehmann explained his role with TSA and the states. He explained he has examined the business practices of Florida, Georgia, Maryland, Pennsylvania, Montana, Texas, California, New Jersey, and Colorado regarding the Hazmat process. TSA plans to visit as many states as possible before the January 2005 deadline. They intend to visit Tennessee, North Carolina, and Illinois to understand the issues regarding Hazmat endorsements.

Next Ms. Cathy Morrison, TSA, provided an update on the TSA Hazmat Program via a conference call. Ms. Morrison explained that her report would be general as TSA is still in the rule making phase. Ms. Morrison provided the following information regarding the TSA Hazmat Program:

- The fee rule has been submitted to the Office of Management and Budget (OMB) and will be sent to the Federal Register for publication.

- The process rule is at OMB. TSA is optimistic that OMB will release a published rule by November 12, 2004. If it is not published by that date then TSA will distribute an exemption form from the current regulation detailing the implementation process.

- TSA intends to award the collection contract by the end of November 2004. The contractor responsibilities will include collecting drivers' applications, fingerprints, fees, and then transmitting them to TSA. The DMVs and state Homeland Security advisors will provide the necessary details for the states to proceed without delay. Approximately 42% of the states, based on driving population, have indicated that they will be performing application, fingerprinting, and fee collection functions themselves. Approximately 29% of the states have yet to determine their preferences.

- TSA anticipates that the initiation fee will not exceed $50.

- TSA is involved in two weekly conference calls with AAMVA. One is a technical conference call and the other is with state representatives from the AAMVA-USA PATRIOT Act working group that discusses policy and/or technical concerns. TSA continues to conduct the state visits and communicates with the states via e-mail.

- TSA has updated its Web site with all the components relevant to the Hazmat program.

Chairman Uzzell requested TSA provide the Council with a state by state template of each state's plan for proceeding and provide a list of states that could be surveyed.
Ms. Morrison explained she would provide the information requested, if possible.

Compact Council Action: **This topic was accepted as information only.**

Topic 4 **Discussion of the Revised Footnote in the State National Fingerprint File (NFF) Qualification Requirements**

Ms. Barron discussed the NFF qualification requirements and explained that during the May 2004 Council meeting, Mr. Mike Timmerman, State Compact Officer from Arizona, raised a question about a footnote included in the NFF qualification requirement 1(a) pertaining to a technical requirement for the states. At that time, Mr. Timmerman explained that when Arizona's candidate name search from a fingerprint submission results in a potential candidate, then Arizona's system verifies the candidate's fingerprints. When the name search yields no potential candidate(s), then Arizona's system automatically forwards the fingerprints to the CJIS Division for a search of the national fingerprint database without a technical search of its automated fingerprint identification system. Mr. Timmerman requested the Council examine this issue and determine if Arizona's technical search policy met the requirements as described in the NFF qualification requirements footnote. In May 2004, the Council

revised the footnote to specify that a technical search of the fingerprints at the state level must be performed prior to submitting the fingerprints to the CJIS Division. In addition, the Council requested that the Standards Committee further examine this state qualification requirement and footnote and provide a recommendation to the Council.

In August 2004, the Standards Committee decided that the suggested revision to the footnote requiring a state technical search should remain as a state NFF qualification requirement. Lt. Larry Burns (proxy for Mr. Timmerman) proposed that the requirement for a state technical search following an unsuccessful candidate search be re-examined.

Compact Council Action: **Lt. Larry Burns made a motion that the Council address Arizona's concerns and look at changing this qualification. There was no second. Motion failed.**

Chairman Uzzell expressed her appreciation to Lieutenant Burns for bringing Arizona's concerns and comments to the Council. She explained that the Council understands the issues facing Arizona and the financial factors involved and will take that into consideration when Arizona begins to participate in the NFF program.

Topic 5 Draft Notice of Approved Methods of Positive Identification for Noncriminal Justice Purposes

Mr. Phillips provided background information regarding the notice for the Council's accepted methods of positive identification. He explained that as a result of legislation and other federal mandates, numerous questions have surfaced regarding what constitutes the definition of positive identification. The CJIS Division's Assistant Director requested that the Council examine this issue and provide clarification regarding the definition of positive identification as defined in the Compact.

At the May 2004 Council meeting, the Council discussed the definition of positive identification relative to noncriminal justice purposes and fingerprint submissions. In addition, the CJIS Division staff briefed the Council regarding the final report of the National Fingerprint-Based Applicant Check Study (N-FACS). The Council approved the following motions at the May 2004 meeting regarding positive identification:

Motion 1 Ms. Uzzell made a motion that the Council define one method of positive identification based on a submission of ten-rolled fingerprints with verification of identification by a comparison of fingerprints. Mr. Rehmann seconded the motion. The motion carried.

Motion 2 Mr. Rehmann made a motion that the Council accept the Standards Committee's recommendation that ten-flat fingerprints comprise another standard for determining positive identification for noncriminal justice purposes so long as the reliability meets or exceeds the CJIS Division's Integrated Automated Fingerprint Identification System (IAFIS) specifications and there is no degradation of IAFIS services. The motion carried.

Motion 3 Mr. Rehmann made a motion that the Council accept the Standards Committee's recommendation to endorse the near-term implementation (within six months) accompanied by a standard for capture devices as explained in the N-FACS report and that the FBI move forward with implementation as long as there is no degradation to IAFIS services. The motion carried.

The Council endorsed future FBI fingerprint pilots, whereby an acceptable scientific reliability may be shown which deviates from the ten-rolled fingerprints and other accepted standards for positive identification. The Council endorsed pilots involving less than ten-rolled fingerprints to be conducted by the CJIS Division in conjunction with the state/agency willing to conduct such pilots. The pilot should produce appropriate statistical and scientific analysis which should be brought before the Council for a discussion of the pilot's merits. Furthermore, the Council concluded that the definition in Article I (20) of the Compact speaks of a "comparison of fingerprints" without specifying how many fingerprint images; therefore, the definition is flexible enough to accommodate any future position the Council may favor concerning using less than ten-rolled or flat fingerprints.

During the May 2004, meeting the Council requested the FBI's Council staff to prepare a draft notice for publication in the Federal Register **(Attachment 5)** explaining the Council's approved methods of positive identification. In August 2004, the Standards Committee reviewed a first draft of the notice and made suggestions and changes for the FBI's Council staff to incorporate. During discussion of the notice, Chairman Uzzell requested that language explaining which standards and/or specification to be used should be referenced in the notice, as well as a federal and state point of contact. The Council considered the following suggestion for the Summary portion of the notice:

SUMMARY**:** At its May 2004 meeting, the Compact Council, established by the National Crime Prevention and Privacy Compact (Compact), approved two methods for determining positive identification [defined in Article I (20) of the Compact] for noncriminal justice purposes. ~~For future updates to the Compact Council's list of approved methods of positive identification for noncriminal justice purposes, interested parties should contact the FBI's Compact Council Office.~~ **Information regarding a state or federal agency's acceptable standards and technical capabilities to process fingerprints should be obtained from the State Compact Officer in a Compact State, the Chief Administrator of the State Central Repository in a non-Compact State, or the FBI Compact Officer.**

The Council agreed to the following change on page 4 of the notice:

"nor shall it degrade the search accuracy and/or computing capacity of the FBI's CJIS Division's Integrated Automated Fingerprint Identification System (IAFIS) **as determined by the FBI CJIS."**

The Council agreed to the following addition on page 4 of the notice:

Future alternatives for determining positive identification of **criminal history record checks** must be coordinated with the FBI's CJIS Division, and the scientific reliability should not significantly deviate from the reliability of ten-rolled fingerprints, ten-flat fingerprints, and other Compact Council accepted methods for positive identification for noncriminal justice purposes.

Mr. Frank Campbell, DOJ, opined that he would like DOJ staff to review the draft notice to determine if it should be published as a rule instead of a notice.

Compact Council Action: **Lt. John O'Brien made a motion that the Council approve the Notice of Approved Methods of Positive Identification for Noncriminal Justice Purposes with the proposed changes and publish it as a proposed notice in the Federal Register with a caveat that if the DOJ decides that it should not be published as a notice then the topic will be readdressed at the next Council Meeting. The motion was seconded by Ms. Debbie McKinney. Motion carried.**

Topic 6 Two-Print Pilot with Department of State (DOS)

Ms. Tracy Pacoe, CJIS Division staff, and Mr. David Boyd, DOS, presented this topic. **(Attachment 6)**

Ms. Pacoe explained the CJIS Division's relationship with DOS as a result of the requirements of the USA PATRIOT Act of 2001, which authorized DOS to receive National Crime Information Center (NCIC) and Interstate Identification Index (III) data extracts from the CJIS Division. DOS imports the III and NCIC data into its Consular Lookout and Support System (CLASS), which is the system that DOS uses to conduct initial name checks of visa applicants at embassies and consulates world wide. In addition, she explained that DOS and the CJIS Division intend to conduct a pilot with the San Salvador consulate that will allow the submission of two fingerprints of visa applicants following an initial check of the Department of Homeland Security's Automated Biometric Identification System (IDENT). If the IDENT check results in a "hit", the San Salvador consulate will electronically submit the two-print fingerprint containing the FBI number obtained from IDENT. Then, the CJIS Division will verify the two-print fingerprint submission with the submitted FBI number and respond electronically to the San Salvador consulate. In addition, she summarized the other ten-print fingerprint pilots with DOS' Mexican consulates as follows:

- Consulates submit to the CJIS Division using different ten-print scanners to submit ten-flat fingerprints (Cuidad Juarez, Mexico City, Monterrey, and Guadalajara)

- Two-print submissions with a quoted FBI Number (San Salvador)

The Council requested additional information regarding the two-print fingerprint pilot with San Salvador. Specifically, the Council requested a time line for completion of the pilot, objectives of the pilot, criteria for evaluation, and an explanation of the CJIS Division and DOS two-print fingerprint pilot

process. Chairman Uzzell thanked the DOS personnel for attending the meeting and encouraged attendance at future meetings to discuss the progress of the fingerprint pilots.

Compact Council Action: **Mr. Frank Sleeter made a motion to endorse the DOS, Bureau of Consular Affairs Two-Print pilot with the understanding that the specific objectives of the pilot including the evaluation criteria, be provided to the Council at the Spring 2005 Council meeting. The motion was seconded by Mr. Paul Heppner. Motion carried.**

Topic 7 User Fee Ad Hoc Committee Report

Lt. Tom Turner, Chairman, User Fee Ad Hoc Committee (Committee), provided an overview of the telephone conference conducted in October 2004. The Committee agreed to study the services provided by states based on the fees collected from applicant fingerprint submissions. The Committee recommended a survey of the states that would focus on its use of fees generated from fingerprint submissions. The National Consortium for Justice Information and Statistics (SEARCH) agreed to assist the Committee with development of the survey and questions. The Committee will review the draft survey questions and request input from the Committee for additional questions before sending the survey to the states in December 2004. The Committee will analyze and evaluate the information provided by the states regarding the fees and provide a report to the Standards Committee and the Council.

Additionally, Mr. Commodore provided clarifying information regarding the FBI's current fingerprint fee. He explained that the processing fee for fingerprints is $24; however, a $2 rebate is awarded when a state agrees to be billed directly by the CJIS Division. The CJIS Division plans to send a letter to contributors that explains the fee schedule.

Compact Council Action: **This topic was accepted as information only.**

Topic 8 Report from National Conference of State Liquor Administrators (NCSLA)

Mr. Commodore explained that the National Conference of State Liquor Administrators (NCSLA) had contacted the CJIS Division about channeling fingerprints on behalf of alcoholic beverage license applicants. Mr. Commodore suggested that the NCSLA address the Council regarding its intentions. Mr. Matt Cook, an officer with NCSLA and director of the State Liquor Enforcement of Colorado, explained that for the past five years, NCSLA has extensively researched the possibility of channeling fingerprints on behalf of its applicants across the United States. Mr. Cook explained that the NCSLA proposal would allow NCSLA to become a channeler on behalf of alcoholic beverage license applicants who seek licensure in the 27 states that are compliant with Public Law 92-544. NCSLA's proposal calls for an NCSLA officer to submit a single set of fingerprints to NCSLA who would submit the fingerprints to the FBI's CJIS Division on their behalf. Any CHRI would be distributed pursuant to established guidelines.

Mr. Wilbur Rehmann requested clarification of NCSLA's intentions. Mr. Cook explained that NCSLA intended to use the Outsourcing rule as authorization to act as the channeling agency; however, in the absence of an Outsourcing rule, NCSLA may consider approaching Congress to pass legislation on its behalf. Mr. Rehmann explained that the Outsourcing rule will not supercede state laws that require fingerprint-based checks at the state level before a national check. After considerable discussion of the issue, Chairman Uzzell agreed to refer this topic to the User Fee Ad Hoc Committee.

Compact Council Action: **Mr. Jerry Pender made a motion to refer this topic to the User Fee Ad Hoc Committee for educational purposes on both sides, so that NCSLA can be educated on what their issues will be and also so that the Council can understand long-term strategy and what they need to be taking into account on further issues that need to be addressed. Mr. Paul Heppner seconded the motion. Motion carried.**

Topic 9 **Standards Committee Report on the Update on the FBI Interstate Identification Index (III) System Policy for Criminal Justice Purpose Name Checks (Purpose Code "C") at Federal Office Buildings and Facilities**

At the October 2003 Council meeting, the Council discussed the CJIS APB policy allowing III name checks of contractors requiring access to federal facilities. In 1996, the CJIS APB authorized the use of Purpose Code "C", criminal justice purposes, to conduct III background name checks of contractors entering federal facilities. This change in policy was made prior to the Compact Act being passed. The Council's Standards Committee discussed the fact that since the enaction of the Compact Act, the use of Purpose Code "C" to conduct III background checks on contractors entering federal facilities as authorized by the CJIS APB policy may need to be reconsidered.

The Standards Committee recommended the formation of a committee comprised of representatives of the CJIS APB and the Council to meet with CJIS Division personnel to discuss the CJIS APB approved policy. The newly formed committee will research this topic and related issues and provide potential alternatives that would be acceptable to both the Council and the CJIS APB.

Compact Council Action: Mr. Jerry Pender made a motion that the CJIS Division staff convene an Ad Hoc working committee with the Compact Council and the CJIS APB to define the criteria that should be used to determine if access to III data falls under the administration of criminal justice or noncriminal justice purposes. The motion was seconded by Mr. Frank Sleeter. Motion carried.

Topic 10 **Sanctions Committee Report**

Ms. Julie LeTourneau, Chairman of the Sanctions Committee, provided an update on the proposed revisions to Title 28, Code of Federal Regulations, Part 905. The Sanctions Committee recommended publishing the Sanctions rule pending the Council's approval.

During the Sanctions Committee meeting on November 2, 2004, the Committee reviewed the recently conducted CHRI audits from eight states based on the proposed Sanctions rule. The Sanctions Committee reviewed the CJIS Audit Unit's (CAU) findings regarding the Compact states and those states that signed a Memorandum of Understanding (MOU) for compliance with the Compact and applicable Council rules. Additionally, the CAU reviewed the NFF states for NFF compliance, as well as other Compact-related compliance issues. Further, the CAU reviewed non-MOU and non-Compact states for compliance with Council rules, which the CJIS Division has adopted for general use. The Sanctions Committee recommended sending letters to the states after a review by Chairman Uzzell. Following CAU's summary of its findings, the Sanctions Committee decided it will report to the Council any serious violations with recommendations on a course of action. Ms. LeTourneau reported that none of the states had any violations that would have required such action.

The Sanctions Committee also reviewed the pilot Noncriminal Justice Agency (NCJA) Audits. Since March 2004, the CAU conducted NCJA Audits of 12 states, the American Bankers Association, including six banking institutions, and five Federal channeling agencies. The CAU agreed to provide the Sanctions Committee with the methodology, the findings of the pilot audits, and evaluations for the Sanctions Committee to make recommendations for the Council to consider before proceeding with the audits.

Compact Council Action: Ms. Julie LeTourneau made a motion to approve the publishing of the Sanctions rule as well as publishing the notice of the NFF audit methodology and the sampling standards. The motion was seconded by Lt. John O'Brien. Motion carried.

Topic 11 Utilizing the Delayed Fingerprint Submission Rule for Federal Emergency Management Agency (FEMA) Criminal History Record Checks

Mr. Danny Moye, FBI OGC, explained that FEMA contacted OGC and explained their need to conduct between 1,000-2,000 background checks of temporary employees to handle natural disasters and emergency situations. Because of the hurricanes in Florida, FEMA needed to hire temporary employees quickly; therefore, they requested the ability to conduct III name-based checks prior to submitting fingerprint-based background checks. Mr. Moye contacted the FBI's Compact Office who contacted the Compact's Executive Committee to explain FEMA's request. The Council's Executive Committee temporarily authorized FEMA's access to III under the scope of the delayed fingerprint submission rule. The CJIS Division established procedures whereby the Federal Protective Service conducted the III name-based check on behalf of FEMA and the fingerprints would be submitted to the CJIS Division by courier on a daily basis, therefore meeting the fifteen day requirement of the rule. Mr. Moye explained that FEMA would be providing a formal request to the Council.

Compact Council Action: Ms. Carole Shelton made a motion to accept the FEMA proposal to utilize the Purpose Code "X" for III Criminal History Record Checks for emergency situations and publish in the form of a notice in the Federal Register. Mr. Robert Finlayson seconded the motion. Motion carried.

Topic 12 **Status Update on the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act of 2003**

Mr. Allen Nash, CJIS Division Staff, provided a status of the PROTECT Act and the pilot program **(Attachment 7)**. In 2003, the President signed into law the PROTECT Act pilot program. The Act requires the U.S. Attorney General to establish a pilot program for volunteer groups to request and obtain state and national fingerprint-based background checks on volunteers. The three organizations participating in the pilot program are the National Mentoring Partnership (NMP), the Boys & Girls Clubs of America (BGCA), and the National Council of Youth Sports (NCYS). The pilot program is scheduled to run from July 29, 2003 to January 31, 2005. The purpose of the pilot program is to evaluate models for conducting criminal history background checks on individuals that work with children, the elderly, and the disabled. The Act consists of two parts, the child safety pilot program and the state pilot program. Three states were initially identified to participate in the state pilot program: Montana, Tennessee, and Virginia. Florida became the fourth participating state as a result of discussions during previous Council meetings and Standards Committee meetings. Florida became a participant to represent the option of disseminating criminal history records to the qualified entity and allowing them to make the fitness determinations. Under the state pilot program, the states are doing the fitness determinations in accordance with their own procedures. Under the child safety pilot program, the FBI provides the criminal history records to the National Center for Missing and Exploited Children (NCMEC). NCMEC also worked with volunteer organizations to develop fitness criteria.

Mr. Nash provided the following accomplishments of the PROTECT Act:

Manual In-Electronic Out - The FBI is sending electronic responses to fingerprint card submissions received manually.

Paper Check Conversion - Organizations now submit a payment check when they submit the fingerprint card. Then, the CJIS Division electronically submits the check to the U.S. Treasury Department. Once the funds are approved, the CJIS Division proceeds with processing the fingerprint submission.

Electronic Submission of fingerprints via LEO - NMP submits fingerprints via Law Enforcement Online (LEO). The fingerprints are submitted electronically via a dial-up connection. A recent technical upgrade to LEO now allows the fingerprints to be transmitted within seconds as opposed to 15 minutes or more before the upgrade.

Record Challenge Process - The PROTECT Act gives every individual who undergoes a background check the right to request a copy of their record and challenge the accuracy and completeness of the information in that record. Previously the individual had to submit a departmental order, which meant they had to submit a separate fingerprint card and its associated fee. In the letter to the applicant, a transaction number is provided along with forms to request a copy of their criminal history record for themselves, the volunteer organization, or both. Approximately 49 of these requests have been received to date.

Mr. Nash discussed a survey sent to the volunteer organizations regarding customer expectations. The volunteer organizations sent the survey to their members. The NCYS provided one response, the BGCA provided approximately 60 responses, and NMP provided approximately 400. The CJIS Division provided the data from the survey to the Bureau of Justice Statistics (BJS) for their expert assistance. BJS has prepared a draft copy of the conclusions, but is waiting for the draft copy to be approved prior to disseminating the results. Mr. Nash advised that a preliminary result indicated that for most volunteer organizations the impediments to fingerprint background checks involves not only a financial cost but also accessibility to fingerprinting mechanisms that create problems for volunteer organizations.

Next, Mr. Nash provided information regarding an Ad Hoc study to examine the accuracy of federal records versus state records and public name checks versus fingerprint-based checks. The Ad Hoc study is ongoing and should be finished by January 31, 2005. Another Ad Hoc study regards providing criminal history records to the qualified entity. SEARCH assisted with a survey involving 24 states that indicated the benefits of disseminating the criminal history information to the qualified entity. In addition, 34 states indicated their preference of having the option of providing criminal history record checks directly to the qualified entities.

Compact Council Action: This topic was accepted as information only.

Topic 13 Discussion on House Bill H.R. 10 "The 9-11 Recommendations Implementation Act"

Chairman Donna Uzzell explained that the H.R. 10 Bill included various legislative issues with at least four that reference CHRI background checks. Section 21-42 of H.R. 10 includes a provision that would require the U.S. Attorney General to establish a pilot program providing employers the ability to request CHRI under applicable state laws authorizing such a request and to provide the CHRI to the employer. Section 21-45 is a provision authorizing the state's Pub. Law 92-544 statutes to be utilized, and when such a statute is absent, the check could be made directly to the FBI. Another section of the bill discusses the establishment of a national clearinghouse for security guard background checks. This clearinghouse would be implemented within one year following the passage of the legislation. Mr. Moye noted that the Compact was not mentioned in the bill as a reference.

Chairman Uzzell contacted the Council's Executive Committee regarding the H.R. 10 Bill and they decided to prepare a written resolution to Congress. However, after consulting with the DOJ, the Executive Committee agreed that Chairman Uzzell would prepare a letter to Congress representing the state of Florida and indicating its concerns regarding the bill.

Mr. Owen Greenspan, SEARCH, provided a status report of the bill in Congress. He explained as of November 1, 2004, the House and Senate had not reached an agreement regarding the establishment of the National Intelligence Director position. Mr. Robert Holloran, National Background Data, commented that the National Association of Professional Background Screeners and the Consumer Data Industry are lobbying very strongly for the H.R. 10 bill to be passed.

Chairman Uzzell discussed the role of the Council and the Compact Act in providing information to Congress regarding potential legislation that involves or is of interest to the Council. Chairman Uzzell discussed the fact that the Council could serve as a valuable resource to Congressional members as they consider legislation that may in fact fall within the purview of the Council's authority. Mr. Campbell, DOJ, explained that he felt if potential legislation appeared to involve the Compact Act and the Council it seems the bill's sponsor is unaware of it, then the Council may justifiably intervene to assist in educating the lawmakers as they proceed with the work on the potential legislation. Further, Chairman Uzzell felt that creating a Council Web site would assist in providing a Web-based forum to obtain Council and Compact Act information.

Compact Council Action: This topic was accepted as information only.

Topic #14 Legislative Update

Mr. Danny Moye, FBI OGC, presented information regarding federal legislation, both pending and current enacted laws, introduced in the 108th Congress that may impact the CJIS Division and its user community. Mr. Moye advised that any questions regarding the legislative update should be referred to him or Ms. Melody Ferrell, FBI OGC.

Mr. Moye discussed HR 218, which authorizes concealed weapons permits for retired and active law enforcement officers. Mr. Moye mentioned that federal and state agency's concerns with this bill are being examined by the DOJ. One of those concerns is what would happen if the retired officer registered in one state moves to another state (i.e., Would the officer be required to undergo another background check?). Mr. Moye advised that III and NCIC would be the only available databases for these background checks and not the National Instant Criminal Background Check System database.

Next, Mr. Gary Barron, CJIS Division staff, discussed the Medicare Prescription Drug and Modernization Act of 2003. Mr. Barron explained that one provision of this act provides for a pilot program to evaluate national and state background checks on direct patient access employees of long-term care facilities. The responsibility for this pilot belongs to the Secretary of Health and Human Services, specifically the Center's for Medicare and Medicaid Services (CMM) Department with assistance from the U.S. DOJ. The act permits the federal government to enter into agreements with up to ten states to conduct the pilot program. The act provides 25 million dollars to implement the pilot and produce a Government Accounting Office report of the pilot in 2007.

The CMM conducted several teleconferences with entities within the states to coordinate the pilot and provide information regarding the process. The CMM distributed a solicitation package for participation that provided the requirements for the pilot. The pilots intend to begin by the end of January 2005.

Compact Council Action: Mr. Paul Heppner made a motion that the Council send out a blanket informational brochure (reviewed and approved by DOJ) to Congressional members to educate them on the Compact and to send personalized letters (reviewed and approved by DOJ) to those who have introduced bills regarding background checks. The motion was seconded by Ms. Carole Shelton. Motion carried.

Topic #15 Status Report on Pending Rules and Notices

Ms. Paula Barron provided a report on the following pending rules and notices.

Record Screening Rule (Attachment 8)

Ms. Barron guided the Council through a review of the comments (shown in highlight/strikeout in the attachment) from the most recent OGC and DOJ review.

Compact Council Action: Mr. David Sim made a motion to revert back to the original language in Section 904.3, State Criminal History Record Screening Standards, of the Records Screening Rule and add "subject to the Compact" after the word "search". The motion was seconded by Ms. Carole Shelton. Motion carried.

The new language will read as follows: The following record screening standards relate to criminal history record information received for noncriminal justice purposes as a result of a national search subject to the Compact utilizing the III system.

Compact Council Action: Mr. Frank Sleeter made a motion to accept and publish the proposed rule for Criminal History Record Screening for Authorized Noncriminal Justice Purposes, including the changes referred to in the above motion regarding Section 904.3. The motion was seconded by Mr. Jerry Pender. Motion carried.

NFF Qualification Requirements Rule and Notice (Attachment 9)

The proposed change for this rule is under Section 905.2 and will provide consistency between language in the rule and that contained in the notice. The following phrase was added, "each NFF program participant will meet the standards set forth in the NFF qualification requirements as established by the Council and endorsed by the FBI's CJIS APB."

Compact Council Action: Ms. Lana Adams made a motion to publish the NFF Qualification Requirements Rule and Notice with one change, the removal of the word "final" from the sentence in the summary section of the notice which will now read, "The Council coordinated the development of the NFF Qualification Requirements with the FBI's CJIS Division staff and forwarded the ~~final~~ document to the CJIS APB for its endorsement prior to publication. The motion was seconded by Mr. Paul Heppner. Motion carried.

Mr. Campbell, DOJ, requested a further review of the NFF rule and notice. Chairman Uzzell requested the FBI's Council staff to proceed with publication in the Federal Register if DOJ does not have substantive comments. The proposed rule and notice should be returned to the Council to consider any substantive comments.

Topic #16 Compact Council Web Site

Chairman Uzzell mentioned the testimony she made to a Congressional subcommittee regarding the Compact Act and the Council. While conducting research for the testimony, she discovered that the limited information available on the internet was outdated and of little value. In addition, Mr. Commodore explained that the issue of a Council World Wide Web (Web) site has been mentioned during previous meetings. There has been past interest from the Council and its members in establishing a Council Web site accessible by all Council members, those from both noncriminal and criminal justice agencies, as well as to the general public. This Web site could include the mission statement of the Council, the Council Bylaws, Council membership list, upcoming meeting information, topic papers, past meeting minutes, current initiatives, Council rules and notifications published in the Federal Register, and historic documentation.

Next, Mr. Commodore reviewed the options available for the Council to consider. The first option would provide a link on the www.fbi.gov Web site that would include Compact Council information. The www.fbi.gov Web site would allow access to personnel from noncriminal and criminal justice agencies, as well as the general public. LEO is another option, however, it would only be available to criminal justice agencies. The SEARCH Web site, www.search.org, is another option for the Council to consider. The final option would be for a state to volunteer as host of the Web site on behalf of the Council.

Mr. Commodore advised that initially time and resources would be expended in establishing a link at the www.FBI.gov Web site, but once established the FBI's Council staff would maintain the site on behalf of the Council. Mr. Commodore explained that LEO could still be utilized and any restricted information would be available via LEO. General public information would be available at the www.fbi.gov Web site.

Compact Council Action: Mr. Paul Heppner made a motion to approve the establishment of a Compact Council web site, utilizing the www.FBI.gov Web site. The motion was seconded by Mr. Jerry Pender. Motion carried.

ADDITIONAL TOPICS

Update on the Rap Sheet Standardization

Mr. John Loverude, former Chairman of the Joint Task Force (JTF) on Rap Sheet Standardization provided an update on the Rap Sheet Standardization project **(Attachment 10)**. Mr. Loverude explained that the objectives of the JTF were to develop a standardized criminal history transmission format, to develop a standardized presentation format, and to develop a concept of operations which combines criminal histories from multiple sources into a single criminal history rap

sheet. Currently, three states and the FBI are participating in this program. Texas intends to implement the standardized rap sheet by the end of 2004 and several other states indicated they are preparing for it.

Mr. Loverude explained that the International Justice and Public Safety Information Sharing Network (NLETS) plans to conduct an Extensible Markup Language (XML) Implementers Conference to assist states and entities implementing the standardized rap sheet. The one day conference is tentatively planned for January 12, 2005. On January 13 and 14, 2005, NLETS will offer assistance with other XML - related implementations.

Compact Council Action: This topic was accepted as information only.

Submitting Name Checks via LEO

Ms. Debbie Chapman, CJIS Division staff, provided information regarding the name check process via LEO and a brief overview on improvements that have been made to the name check process. **(Attachment 11)**

In June 2004, additional information was added to the L0008 error message. This change provides a clear indication when candidates are found in IAFIS processing. If candidates were there but were not able to be idented or non-idented, the FBI wanted to return this information to the contributors so they would know that another fingerprint card was needed. A name check request form is now available on LEO, and is located under LEOSIG, PUBLIC SIG, CJIS, PROGRAMS, III and then On-Line Name search Form. Responses are returned via LEO to the point of contact that is provided on the original request. Name check requests were previously only accepted via mail or fax.

Just under 4,000 name checks are done on an average month. Ninety-nine percent are completed on the day of the request and the Ident rate is 1.71 percent.

Compact Council Action: This topic was accepted as information only.

OTHER BUSINESS

Chairman Uzzell mentioned that the Executive Committee will consist of the chairs of the other Council committees which include Mr. David Sim, the Vice-chair of the Council and chair of the Dispute Adjudication Committee, Mr. Paul Heppner, chair of the Standards Committee, and Ms. Julie LeTourneau, chair of the Sanctions Committee. The Executive Committee will review the committee membership and update their member list to fill vacancies. Chairman Uzzell said that her goal is to fill committee openings with as many State Compact Officers as possible who do not sit on the Council.

The meeting was adjourned at 12:08 p.m.

Compact Council Meeting Attendee List
Denver, Colorado
November 3-4, 2004

Lana K. Adams	Office of Personnel Management
Nancy Altman	Department of State
Gary Barron	FBI
Paula Barron	FBI
Curtis Bass	Mississippi Department of Public Safety
David Bolme	Identix Identification Services
David J. Boyd	Department of State
Wendy L. Brinkley	North Carolina State Bureau of Investigation
Larry Burns	Arizona Department of Public Safety
Frank Campbell	U.S. Department of Justice
Debbie M. Chapman	FBI
Todd C. Commodore	FBI
Jan Dempsey	Colorado Bureau of Investigation
Stacye Dorrington	Montana Department of Justice
Robert M. Finlayson, III	Georgia Department of Human Resources
Jonathan Frenkel	Department of Homeland Security
Cora Gentry	Arkansas State Police
James P. Gray	FBI
Owen Greenspan	SEARCH
Paul C. Heppner	Georgia Bureau of Investigation
Robert Holloran	National Background Data
Jeffrey R. Kellett	New Hampshire State Police

Lori Kemp	FBI
James E. Kessler, Jr.	Wachovia Corporation
Lisa Knight	Hunter + Geist
Eric M. Lapp	National Background Check
Adrienne Leach	FBI
Julie LeTourneau	Minnesota Bureau of Criminal Apprehension
John Loverude	Advanced Technology Systems
Angell Magnani	Iowa Department of Public Safety
William L. Marosy	U.S. OPM-CFIS
Scott Martin	Connecticut State Police
Timothy P. McGrail	Missouri State Highway Patrol
Robert W. McKeever	Maryland Department of Public Safety (Retired)
Debbie S. McKinney	Oklahoma State Bureau of Investigation
Glen W. McNeil	Sagem Morpho
Tina Medich	California Department of Justice
Kathryn M. Monfreda	Alaska Department of Public Safety
Liane M. Moriyama	Hawaii Criminal Justice Data Center
Danny Moye	FBI
Teresa Mucha	Colorado Bureau of Investigation
Allen Wayne Nash	FBI
Mary Neff	Washington State Patrol
John H. O'Brien	New Jersey Division of State Police
Tracy L. Pacoe	FBI
Kimberly Parsons	FBI
Jerome Pender	FBI

Scott S. Phillips	FBI
Wilbur Rehmann	Montana Department of Justice
Pam Ritchey	Iowa Department of Public Safety
David Rocchio	Colorado Bureau of Investigation
Carole Shelton	Maryland Department of Public Safety and Correctional Services
David G. Sim	Kansas Bureau of Investigation
Cynthia Simers	FBI
Frank G. Sleeter	Sun Prairie Police Department
Kimberly K. Smith	FBI
Carlotta C. Stackhouse	South Carolina Law Enforcement Division
Don Starney	Colorado Bureau of Investigation
June Still	Tennessee Bureau of Investigation
Richard J. Thomas	Appriss
Thomas Turner	Virginia State Police
Donna M. Uzzell	Florida Department of Law Enforcement
Delbert W. Watkins, II	National Visa Center
Barbara S. Wiles	FBI
Jonathan D. Williams	FBI
Erik Wolle	Identix Identification Services
Paul Woodard	SEARCH

Compact Council Meeting
November 3-4, 2004
Denver, CO
Topic #1

Establishment of Minimum Standards for Verifying the Identity of Applicants When Being Fingerprinted

Standards Committee Recommendation

In August 2004, the Standards Committee asked FBI Council Staff to research this topic further and provide information to the Council and the Committee.

The Council's Goals

- To establish, at a minimum, guidelines, recommendations, etc., to limit applicants from using fraudulent identification forms, or other aberrant practices when being fingerprinted for noncriminal justice background checks

The Council's Goals

- Forward a comprehensive report to the Standards Subcommittee for review and comment
- Establish "best practices" for fingerprinting applicants for noncriminal justice background checks

Identification and Verification

- What is the definition of each term?
- How do they apply to the issue of establishing a fingerprint applicant's identity?

Identification & Verification

- **Identification** is the term used to describe the process of matching a biometric (fingerprints, facial recognition) record from a single subject probe against an entire database of similar biometric records in order to determine the identity of the owner of the biometric record.

Identification & Verification

- **Verification** is the term used to describe the process of confirming that a person is who he/she claims to be by matching their biometric record against that of their claimed identity.

Standards Committee Research Plan

- Examine Current Work in the area of Verifying Identification Documents
- Examine Examples of Current Applicant Fingerprinting Procedures
- Establish a Chain of Custody for Applicant Fingerprinting
- Establish Minimum Standards for the Committee and the Council to Review and Recommend "best practices"

Research Results

What was discovered regarding the issue of Establishing and Verifying a Fingerprint Applicant's Identity?

Development of Standard Identification Cards for Verifying Identity

- AAMVA – Uniform Driver's License (UDL)
- Department of Defense – Common Access Card (CAC)
- Federal Government – Federal Personal Identity Verification Standard

AAMVA's Uniform Driver's License

- Development of the UDL
  - Input from across the country to create a specification
  - Common Security feature
  - Various Pilot projects that test interoperability between different agencies and the DMV's using the DL, digital photos and other developing technologies
  - Verification matrix

The UDL and a National Identification Card

- Opposition by many groups to the use of the UDL as a National ID card
- IACP Endorsement

DOD Common Access Card (CAC)

- Investigating multiple architectural solutions for matching and storing biometrics
- Exploring the impact of using encryption technology
- Researching a contactless environment

Federal Government – Personal Identity Verification Standard for Federal Employees and Contractors

- Executive Office of the President urged a cross-agency approach for authentication and identity management
- Homeland Security Presidential Directive HSPD-12– Committee to develop Personal Identity Verification Standards by February 28, 2005
- http://csrc.nist.gov/piv-project

Examples of Different Models for Fingerprinting Practices and Verifying an Applicant's Identity

California

DHS

Federal Legislation

California

- Statutory Authority – To establish, implement and maintain a certification program to process fingerprint-based criminal offender record information background checks on individuals who fingerprint applicants for licensure, certification, or employment purposes
- Requires employees to be certified, if not a law enforcement employee or other state employee already trained in taking fingerprints.

California

- Fingerprint Rolling Certification Program – Reference Handbook for Employees
  - Describes Processing Procedures for the Fingerprint Rolling Certification Program
  - Describes procedures for the employee's responsibilities
  - Provides for the use of a confidential certification number for employees
  - Provides procedures for validating a person's identity
  - Contains a pamphlet titled "Is It Valid?"

DHS Model- United States Citizenship and Immigration Services (USCIS)

- Immigrant fingerprinting
- Nationwide Immigration Field Offices
  - Established Operational Policies and Procedures for Fingerprinting
  - Detailed role of each individual employee in the process

DHS Model – The USCIS Standard Procedures Includes

- Written procedures for each step in the immigrants fingerprinting process (manual and Live Scan fingerprinting)
- "Identity Confirmed" on the appointment notice
- Specific employee functions for fingerprinting immigrant applicants (Fingerprint Technician, Quality Assurance, Supervisor)
- System training specific to CIS technology

DHS Model

- The QA's role is to verify the applicant's identity by:
  - Comparing the picture id to the applicant by comparing facial type, bone structure, skin color and texture, ear size, neck size, eye color and size, nose size, shape of mouth, forehead size, and lip size and shape
  - Verifying the accuracy of DOB with other applicant documents
  - Verifying the signature is the same as one of the names listed on the fingerprint submission

Federal Legislation

- PROTECT Act – The individual volunteering is responsible for providing:
  - A set of fingerprints
  - Name, address, and DOB as it appears on a document made or issued by or under the authority of the US Government, a State, political subdivision of a State, a foreign government, a political subdivision of a foreign government, an international governmental or an international quasi-governmental organization
  - A photocopy of the document described above
  - A statement of whether he/she has a criminal record and, if so, the particulars of such record

Federal Legislation

- Flight Training Candidates Checks Program (FTCCP)
  - The candidate must confirm his/her identity to the fingerprinting entity by providing his/her Passport and one of the following:
    - Resident alien card
    - A valid US driver's license

Chain of Custody

- Why it is important
  - To ensure the individual being fingerprinted is the person he/she claims to be
- Potential pitfalls
  - No central fingerprint collection point
  - Forms for the fingerprint technician to record the applicant's name, address and documents used to verify the identity of the applicant – subject to forgery
  - Space limitations on the FBI fingerprint card
  - Uniform rules for taking fingerprints – international and national

Fraudulent Document Recognition Model Training Program

- Provides a comprehensive modular training program to train motor vehicle and law enforcement employees in verifying the quality/validity of specific identification documents they encounter during the execution of their duties

Questions?

BILLING CODE: 4410-02P

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

28 CFR Part 906

[NCPCC 107]

Outsourcing of Noncriminal Justice Administrative Functions

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Proposed Rule.

SUMMARY: The Compact Council, established pursuant to the National Crime Prevention and Privacy Compact (Compact), is publishing a proposed rule to permit the outsourcing of noncriminal justice administrative functions involving access to criminal history record information (CHRI). Procedures established to permit outsourcing are required to conform with the Council's interpretation of Articles IV and V of the Compact.

DATE: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Send all written comments concerning this proposed rule to the Compact Council Office, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306; Attention: Todd C. Commodore. Comments may also be submitted by fax at (304) 625-5388 or by electronic mail at tcommodo@leo.gov. To ensure proper handling, please reference "Noncriminal Justice Outsourcing Docket No. 107" on your correspondence. You may view an electronic version of this proposed rule at www.regulations.gov. You may also comment via electronic mail at tcommodo@leo.gov or by using the www.regulations.gov

comment form for this regulation. When submitting comments electronically you must include NCPPC Docket No. 107 in the subject box.

FOR FURTHER INFORMATION CONTACT: Ms. Donna M. Uzzell, Compact Council Chairman, Florida Department of Law Enforcement, 2331 Philips Road, Tallahassee, Florida 32308-5333, telephone number (850) 410-7100.

SUPPLEMENTARY INFORMATION: The National Crime Prevention and Privacy Compact (Compact), 42 U.S.C. 14616, establishes uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes. The Compact was approved by the Congress on October 9, 1998, (Pub.L. 105-251) and became effective on April 28, 1999, when ratified by the second state. Article VI of the Compact provides for a Compact Council that has the authority to promulgate rules and procedures governing the use of the Interstate Identification Index (III) System for noncriminal justice purposes. This proposed rule will permit a third party to perform noncriminal justice administrative functions relating to the processing of CHRI maintained in the III System, subject to appropriate controls, when acting as an agent for a governmental agency or other authorized recipient of CHRI.

The rulemaking process established by the Council provides an opportunity for comments through the publishing of a proposed rule. Accordingly, interested persons are invited to participate in this rulemaking by submitting written data, views, or arguments. In addition to this opportunity for comments, the foundation for the concept, merits and wisdom as outlined in this proposed rule has been debated at meetings open to the public. Further, prior

public notice is given in the Federal Register of each Council meeting, including the matters to be addressed at the meeting. Therefore, there is public opportunity to comment on the merits of proposed rules.

In recent years, government and other statutorily authorized entities seeking improved efficiency and economy have become increasingly interested in permitting third party support services for noncriminal justice administrative functions. This is due in large part to the escalating demand for fingerprint-based risk assessments for authorized licensing, employment and national security purposes over the last several years. The escalating numbers of noncriminal justice fingerprint submissions has resulted in increased workloads for local, state, and federal government entities. Coincidentally, under OMB Circular No. A-76, the federal government is encouraged wherever feasible to use private sector services.

The Compact requires the FBI and each Party State to comply with III System rules, procedures, and standards duly established by the Council concerning record dissemination and use, system security, and privacy protection. In that regard, the Compact specifies that any record obtained may be used only for the official purposes for which the record was requested. The Compact Council does not believe that the use of private contractors to perform noncriminal justice administrative functions requiring access to CHRI is prohibited provided there are appropriate controls expressly preserving the sole official purpose of the record request. With appropriate standards and requirements, the benefits of outsourcing may be attained without degradation to the security of the national III System of criminal records. For example, under the proposed rule, subject to some exceptions, contracting agencies or

organizations shall not be permitted to have direct access to the III System by computer terminal or other automated means which would enable them to initiate record requests. Further, the proposed rule provides that tasks necessary to perform noncriminal justice administrative functions would be monitored to assure the integrity and security of such records. Under the proposed rule, safeguards would be required to ensure that private contractors may not access, modify, use, or disseminate such data in any manner not expressly authorized by a government agency or a statutorily authorized recipient of CHRI. Such procedures would establish conditions on the use of the CHRI and would limit dissemination of the CHRI to ensure that such CHRI is used only for authorized purposes. Such procedures would also provide for accurate and current data distribution and require proper maintenance and handling, including the removal and destruction of obsolete or erroneous information that has been brought to its attention. These conditions are necessary to ensure the confidentiality of such information.

Further, this proposed rule seeks to permit outsourcing of noncriminal justice administrative functions authorized under Articles IV and V of the Compact. Article IV provides generally for authorized record disclosure; Article V provides record request procedures as related to noncriminal justice criminal history record checks pursuant to the Compact. This proposed rule outlines the basic structured framework for minimum standards to ensure that outsourced contracts satisfy the security and privacy required by the Compact Council when criminal history record checks of the III are conducted for noncriminal justice purposes. The contracting parties are not at liberty to supercede these minimum standards with

lesser standards; however, contracting parties are free to adopt more stringent standards than required by this regulation.

Administrative Procedures and Executive Orders

Administrative Procedures Act

This rule is published by the Compact Council as authorized by the National Crime Prevention and Privacy Compact (Compact), an interstate and Federal-State compact which was approved and enacted into law by Congress pursuant to

Pub. L. 105-251. The Compact Council is composed of 15 members (with 11 state and local governmental representatives). The Compact specifically provides that the Council shall prescribe rules and procedures for the effective and proper use of the III System for noncriminal justice purposes, and mandates that such rules, procedures, or standards established by the Council be published in the Federal Register. *See* 42 U.S.C. 14616, Articles II(4), VI(a)(1) and VI(e). This publication complies with those requirements.

Executive Order 12866

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 12866 is not applicable.

Executive Order 13132

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 13132 is not applicable. Nonetheless, this rule fully complies with the intent that the national government should be

deferential to the States when taking action that affects the policymaking discretion of the States.

Executive Order 12988

The Compact Council is not an executive agency or independent establishment as defined in 5 U.S.C. 105; accordingly, Executive Order 12988 is not applicable.

Unfunded Mandates Reform Act

Approximately 75 percent of the Compact Council members are representatives of state and local governments; accordingly, rules prescribed by the Compact Council are not Federal mandates. Accordingly, no actions are deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

The Small Business Regulatory Enforcement Fairness Act (Title 5, U.S.C. 801-804) is not applicable to the Council's rule because the Compact Council is not a "Federal agency" as defined by 5 U.S.C. 804(1). Likewise, the reporting requirement of the Congressional Review Act (Subtitle E of the Small Business Regulatory Enforcement Fairness Act) does not apply. See 5 U.S.C. 804.

List of Subjects in 28 CFR Part 906

Administrative practice and procedure, Intergovernmental relations, Law Enforcement, Privacy.

Accordingly, chapter IX of title 28 Code of Federal Regulations is amended by adding part 906 to read as follows:

PART 906 - OUTSOURCING OF NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

Sec.

906.1 Purpose and authority.

906.2 Third Party Handling of Criminal History Record Information.

Authority: 42 U.S.C. 14616

§ 906.1 Purpose and authority.

The purpose of this part 906 is to establish rules and procedures for third parties to perform noncriminal justice administrative functions involving access to Interstate Identification Index (III) information. The Compact Council is establishing this rule pursuant to the National Crime Prevention and Privacy Compact (Compact), title 42, U.S.C., chapter 140, subchapter II, section 14616. The scope of this rule is limited to noncriminal justice background checks in so far as they are governed by the provisions of the Compact as set forth in 42 U.S.C. sections 14614 and 14616.

§ 906.2 Third Party Handling of Criminal History Record Information

(a) Except as prohibited in paragraph (b), criminal history record information obtained from the III System for noncriminal justice purposes may be made available:

(1) To a governmental agency pursuant to a contract or agreement under which the agency performs activities or functions for another governmental agency that is authorized to

obtain criminal history record information by a federal statute, federal executive order or a state statute that has been approved by the United States Attorney General; and

(2) To a private contractor, or other nongovernmental entity or organization, pursuant to a contractual agreement under which the entity or organization performs activities or functions for a governmental agency authorized to obtain criminal history record information as identified in paragraph (a)(1) or for a nongovernmental entity authorized to obtain such information by federal statute or executive order.

(b) Criminal history record information provided in response to fingerprint-based III System record requests initiated by authorized governmental agencies or nongovernmental entities for noncriminal justice purposes may be made available to contracting agencies or organizations manually or electronically for such authorized purposes. Such contractors, agencies, or organizations shall not be permitted to have direct access to the III System by computer terminal or other automated means which would enable them to initiate record requests, provided however, the foregoing restriction shall not apply with respect to (1) persons, agencies, or organizations that may enter into contracts with the FBI or State criminal history record repositories for the performance of authorized functions requiring direct access to criminal history record information; and (2) any direct access to records 42 U.S.C. § 14614(b).

(c) The contracts or agreements authorized by paragraphs (a)(1) and (a)(2) shall specifically describe the purposes for which criminal history record information may be made available to the contractor and shall incorporate by reference a security and management

control outsourcing standard approved by the Compact Council after consultation with the United States Attorney General. The security and management control outsourcing standard shall specifically authorize access to criminal history record information; limit the use of the information to the purposes for which it is provided; prohibit retention and/or dissemination of the information except as specifically authorized in the security and management control outsourcing standard; ensure the security and confidentiality of the information; provide for audits and sanctions; provide conditions for termination of the contractual agreement; and contain such other provisions as the Compact Council, after consultation with the United States Attorney General, may require.

(d) The exchange of criminal history record information with an authorized governmental or nongovernmental entity or contractor pursuant to this part is subject to cancellation for use, retention or dissemination of the information in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the Compact Council in consultation with the United States Attorney General.

Dated: _____ _____

Donna M. Uzzell

Compact Council Chairman

BILLING CODE 4410-02P

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

Security and Management Control Outsourcing Standards

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Notice of approval of the Security and Management Control Outsourcing Standards.

Authority: 42 U.S.C. 14616

SUMMARY: Pursuant to title 42, United States Code, 14616, Article VI(e), and title 28, Code of Federal Regulations (CFR), chapter IX, the Compact Council (Council), established by the National Crime Prevention and Privacy Compact (Compact) Act of 1998, approved the attached Security and Management Control Outsourcing Standards (Outsourcing Standards). (See proposed rule "Outsourcing of Noncriminal Justice Administrative Functions," published in today's Federal Register, which is to be codified at 28 CFR Part 906). The Council coordinated the development of the Outsourcing Standards with the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Division staff and CJIS Advisory Policy Board subcommittees. Hereafter, prior to utilizing the Outsourcing Standards, interested parties should request the most current version by contacting the Compact Council Office, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306, Attention: FBI Compact Officer.

FOR FURTHER INFORMATION CONTACT: Todd C. Commodore, FBI CJIS Division, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306; Telephone (304) 625-2803; e-mail tcommodo@leo.gov; fax number (304) 625-5388.

SUPPLEMENTARY INFORMATION: The Council developed two Outsourcing Standards, one for Contractors having access to criminal history record information (CHRI) on behalf of an authorized

recipient for noncriminal justice purposes and one for Contractors serving as channelers of noncriminal justice criminal history record check requests and results. The first Outsourcing Standard ("Security and Management Control Outsourcing Standard for Contractors Having Access to CHRI on Behalf of an Authorized Recipient for Noncriminal Justice Purposes") will be used by Contractors authorized to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI's CJIS Wide Area Network (WAN). The second Outsourcing Standard ("Security and Management Control Outsourcing Standard for Channelers Only") will be used by Contractors authorized access to CHRI through a direct connection to the FBI's CJIS WAN. The two Outsourcing Standards are printed below:

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD

FOR

CONTRACTORS HAVING ACCESS TO CRIMINAL HISTORY RECORD INFORMATION ON BEHALF OF AN AUTHORIZED RECIPIENT FOR NONCRIMINAL JUSTICE PURPOSES

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks and facilities supporting and/or acting on behalf of the Authorized Recipient of CHRI.

1.0 Definitions

1.01 ACCESS TO CHRI means to use, exchange, retain/store, or view CHRI obtained from the III system but excludes direct access to the III system by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).

1.02 AUTHORIZED RECIPIENT means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice

purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

1.03 CHIEF ADMINISTRATOR, as referred to in Article I(2)(B) of the Compact, means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository.

1.04 CHRI, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

1.05 CRIMINAL HISTORY RECORD CHECK, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.

1.06 COMPACT OFFICER, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

1.07 CONTRACTOR means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.

1.08 DISSEMINATION means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

1.09 NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

1. Making fitness determinations/recommendations
2. Obtaining missing dispositions
3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statue approved by the United States Attorney General
4. Other authorized activities relating to the general handling, use, and storage of CHRI

1.10 NONCRIMINAL JUSTICE PURPOSES, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment

suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

1.11 OUTSOURCING STANDARD means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. The Outsourcing Standard authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.

1.12 PHYSICALLY SECURE LOCATION means a location where access to CHRI can be obtained, and adequate protection is provided to prevent any unauthorized access to CHRI.

1.13 POSITIVE IDENTIFICATION, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints[1] or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other nonunique

[1] The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning qualifying fingerprint submissions may be obtained from the FBI Compact Council office.

identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

1.14 PUBLIC CARRIER NETWORK means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

1.15 SECURITY VIOLATION means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 Responsibilities of the Authorized Recipient

2.01 Prior to engaging in outsourcing any noncriminal justice functions, the Authorized Recipient shall request and receive written permission from (A) the State Compact

Officer/Chief Administrator[2] or (B) the FBI Compact Officer.[3] The Authorized Recipient shall provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of the contract as requested. The Authorized Recipient shall inquire whether a prospective Contractor has any security violations (See Section 8.04) and report those findings to the Compact Officer/Chief Administrator prior to outsourcing noncriminal justice administrative functions.

2.02 The Authorized Recipient shall execute a contract prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.

2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact

---

[2]The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to triennially audit each Contractor and Authorized Recipient engaging in outsourcing with the first of such audits to be conducted within one year of the signing of the contract.

[3]State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; maintain up-to-date records of Contractor personnel who have access to CHRI; and ensure that Contractor personnel comply with this Outsourcing Standard.

a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required of the Authorized Recipient's personnel having similar access.[4]

b. The Authorized Recipient shall ensure that the Contractor maintains site security.

c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract and/or Option renewal.

2.04 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that a compliance review was conducted with the Contractor within 90 days of execution of the contract.

2.05 The Authorized Recipient shall provide written notice of any early voluntary termination

[4]If a national criminal history record check of government personnel having access to CHRI is mandated by a state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives.

of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 Responsibilities of the Contractor

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop and document a security program to comply with the current Outsourcing Standard and any revised or successor Outsourcing Standard. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard, the associated Security Training Program, and the reporting guidelines for documenting and communicating security violations and corrective actions to the Authorized Recipient. The Security Program shall be subject to the approval of the Authorized Recipient.

3.03 The Contractor shall be accountable for the management of the Security Program. The Contractor shall be responsible for reporting all security violations of this Outsourcing Standard to the Authorized Recipient.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. Immediate training shall be provided upon receipt of notice on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the

Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall certify to the Authorized Recipient that the annual refresher training was completed for those Contractor personnel with access to CHRI. The Security Training Program shall be subject to the approval of the Authorized Recipient.

3.05 The Contractor shall make its facilities available for announced and unannounced security inspections performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council. Such facilities are also subject to triennial audits by the state and the FBI on behalf of the Compact Council. An audit may also be conducted on a more frequent basis.

3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.

3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill their contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.

3.08 The Contractor shall maintain a log of any dissemination of CHRI.

4.0 Site Security

4.01 The Authorized Recipient shall ensure that the Contractor site is a physically secure location at all times to protect against any unauthorized access to CHRI.

5.0 Dissemination

5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) the Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

6.0 Personnel Security

6.01 If a local, state, or federal written standard requires a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's employees having access to CHRI. The criminal history record check of Contractor employees at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.

6.02 If a local, state, or federal written standard requires a criminal history record check for support personnel, contractors, and custodial workers who work in a physically secure location, then a criminal history record check shall be required for these individuals, unless these individuals are escorted by authorized personnel at all times. The criminal

history record check for these individuals at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's support personnel, contractors, and custodial workers performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.

6.03 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm that each employee understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities.

6.04 If a criminal history record check is required, the Contractor shall maintain a list of personnel who successfully completed the criminal history record check.

7.0 System Security

7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy as they are made known to the Contractor by the Authorized Recipient.

a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.

7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

a. CHRI shall be stored in a physically secure location.

b. The Authorized Recipient shall ensure that a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient must be identified by an ORI or state assigned identifier, and each Contractor or sub-Contractor must be uniquely identified.

8.0 Security violations

8.01 Duties of the Authorized Recipient and Contractor

a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.

b. Pending investigation, the Contractor shall immediately suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

c. The Contractor shall immediately notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI

made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

d. The Authorized Recipient shall immediately notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

8.02 Termination of the contract by the Authorized Recipient for security violations

a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.

b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.

c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.

8.03 Suspension or termination of the exchange of CHRI for security violations

a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 C.F.R. §906.2(d).

b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be immediately deleted or returned as specified by the Authorized Recipient.

8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:

a. The termination of a contract for security violations.

b. Security violations involving the unauthorized access to CHRI.

c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 Miscellaneous provisions

9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.

9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) the CJIS Security Policy.

9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.[5]

9.04 The minimum security measures as outlined in this Outsourcing Standard may only be

[5]Such conditions could include additional audits, fees, or security requirements.

modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.

9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.

9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer

1000 Custer Hollow Road

Module C 3

Clarksburg, WV 26306

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD

FOR

CHANNELERS ONLY

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or

unauthorized access to or modification of information."

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks and facilities supporting and/or acting on behalf of the Authorized Recipient of CHRI.

1.0 Definitions

1.01 ACCESS TO CHRI means to use, exchange, retain/store, or view CHRI obtained from the III system but excludes direct access to the III system by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).

1.02 AUTHORIZED RECIPIENT means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice

purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

1.03 AUTHORIZED RECIPIENT'S INFORMATION SECURITY OFFICER means the individual who shall ensure technical compliance with all applicable elements of this Outsourcing Standard.

1.04 CHIEF ADMINISTRATOR, as referred to in Article I(2)(B) of the Compact, means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository.

1.05 CHRI, as referred in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

1.06 CRIMINAL HISTORY RECORD CHECK, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.

1.07 CJIS SYSTEMS AGENCY, as provided in Section 1.4 of the FBI Criminal Justice Information Services (CJIS) Division's Advisory Policy Board Bylaws, means a criminal justice agency which has overall responsibility for the administration and usage

of CJIS Division Programs within a state, district, territory, or foreign country. This includes any federal agency that meets the definition and provides services to other federal agencies and/or whose users reside in multiple states or territories.

1.08 CJIS SYSTEMS OFFICER, as provided in Section 1.5 of the CJIS Advisory Policy Board Bylaws, means the individual employed by the CJIS Systems Agency who is responsible for monitoring system use, enforcing system discipline and security, and assuring that CJIS operating procedures are followed by all users as well as other related duties outlined by the user agreements with the FBI's CJIS Division. (This title was formerly referred to as the Control Terminal Officer or the Federal Service Coordinator).

1.09 COMPACT OFFICER, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

1.10 CONTRACTOR means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI. Under this Outsourcing Standard applicable to channelers, a Contractor includes one who has direct connectivity to the CJIS Wide Area Network

(WAN) for the purpose of electronic submission of fingerprints to and the receipt of CHRI from the FBI on behalf of an Authorized Recipient.

1.11 CONTRACTOR'S SECURITY OFFICER means the individual accountable for the management of the Contractor's security program.

1.12 DISSEMINATION means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

1.13 NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

1. Making fitness determinations/recommendations
2. Obtaining missing dispositions
3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statue approved by the United States Attorney General
4. Other authorized activities relating to the general handling, use, and storage of CHRI

1.14 NONCRIMINAL JUSTICE PURPOSES, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment

suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

1.15 OUTSOURCING STANDARD means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. The Outsourcing Standard authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.

1.16 PHYSICALLY SECURE LOCATION means a location where access to CHRI can be obtained, and adequate protection is provided to prevent any unauthorized access to CHRI.

1.17 POSITIVE IDENTIFICATION, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints[6] or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other nonunique

[6] The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning qualifying fingerprint submissions may be obtained from the FBI Compact Council office.

identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

1.18 PUBLIC CARRIER NETWORK means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

1.19 SECURITY VIOLATION means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 Responsibilities of the Authorized Recipient

2.01 Prior to engaging in outsourcing any noncriminal justice functions, the Authorized Recipient shall request and receive written permission from (A) the State Compact

Officer/Chief Administrator[7] or (B) the FBI Compact Officer.[8] The Authorized Recipient shall provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of the contract as requested. The Authorized Recipient shall inquire whether a prospective Contractor has any security violations (See Section 8.04) and report those findings to the Compact Officer/Chief Administrator prior to outsourcing noncriminal justice administrative functions.

2.02 The Authorized Recipient shall execute a contract prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.

2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact

---

[7]The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to triennially audit each Contractor and Authorized Recipient engaging in outsourcing with the first of such audits to be conducted within one year of the signing of the contract.

[8]State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; maintain up-to-date records of Contractor personnel who have access to CHRI; and ensure that Contractor personnel comply with this Outsourcing Standard.

a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required of the Authorized Recipient's personnel having similar access.[9]

b. The Authorized Recipient shall ensure that the Contractor maintains site security.

c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract and/or Option renewal.

d. The Authorized Recipient shall ensure that the Contractor establishes and administers an Information Technology (IT) Security Program.

e. The Authorized Recipient shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of,

[9]If a national criminal history record check of government personnel having access to CHRI is mandated by a state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives.

its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.

2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that a compliance review was conducted with the Contractor within 90 days of execution of the contract.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

2.07 The Authorized Recipient shall appoint an Information Security Officer. The Authorized Recipient's Information Security Officer shall:

a. Serve as the security POC for the FBI CJIS Division Information Security Officer;

b. Document technical compliance with this Outsourcing Standard; and

c. Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the CJIS Systems Officer and the FBI CJIS Division Information Security Officer.

3.0 Responsibilities of the Contractor

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules,

procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop and maintain an IT security program. The Contractor is therefore responsible to set, maintain, and enforce the following:

a. Standards for the selection, supervision, and separation of personnel who have access to CHRI.

b. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CHRI.

3.03 The Contractor shall develop and document a security program to comply with the current Outsourcing Standard and any revised or successor Outsourcing Standard. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard, the associated Security Training Program, and the reporting guidelines for documenting and communicating security violations and corrective actions to the Authorized Recipient. The Security Program shall be subject to the approval of the Authorized Recipient.

3.04 The Contractor shall be accountable for the management of the Security Program. The Contractor shall be responsible for reporting all security violations of this Outsourcing Standard to the Authorized Recipient.

3.05 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. Immediate training shall be

provided upon receipt of notice on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall certify to the Authorized Recipient that the annual refresher training was completed for those Contractor personnel with access to CHRI. The Security Training Program shall be subject to the approval of the Authorized Recipient.

3.06 The Contractor shall make its facilities available for announced and unannounced security inspections performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council. Such facilities are also subject to triennial audits by the state and the FBI on behalf of the Compact Council. An audit may also be conducted on a more frequent basis.

3.07 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.

3.08 The Contractor shall maintain CHRI only for the period of time necessary to fulfill their contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.

3.09 The Contractor shall maintain a log of any dissemination of CHRI.

4.0 Site Security

4.01 The Authorized Recipient shall ensure that the Contractor site is a physically secure location at all times to protect against any unauthorized access to CHRI.

4.02 All visitors to computer centers and/or terminal areas shall be escorted by authorized personnel at all times.

5.0 Dissemination

5.01 Only employees of the Contractor, employees of the Authorized Recipient, and such other persons as may be granted authorization by the Authorized Recipient shall be permitted access to the system.

5.02 The Contractor shall maintain appropriate and reasonable quality assurance procedures.

5.03 Access to the system shall be available only for official purposes consistent with the appended contract. Any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.

5.04 Information contained in or about the system will not be provided to agencies other than the Authorized Recipient or another entity which is specifically designated in the contract.

5.05 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

5.06 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) the Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

5.07 The Contractor shall protect against any unauthorized persons gaining access to the equipment, any of the data, or the operational documentation for the system. In no event shall copies of messages or CHRI be disseminated other than as contracted and governed by this Outsourcing Standard.

5.08 All access attempts are subject to recording and routine review for detection of inappropriate or illegal activity.

5.09 The Contractor's system shall be supported by a well-written contingency plan.

6.0 Personnel Security

6.01 If a local, state, or federal written standard requires a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's employees having access to CHRI. The criminal history record check of Contractor employees at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.

6.02 If a local, state, or federal written standard requires a criminal history record check for support personnel, contractors, and custodial workers who work in a physically secure location, then a criminal history record check shall be required for these individuals, unless these individuals are escorted by authorized personnel at all times. The criminal history record check for these individuals at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's support personnel, contractors, and custodial workers performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.

6.03 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm that each employee understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities.

6.04 If a criminal history record check is required, the Contractor shall maintain a list of personnel who successfully completed the criminal history record check.

7.0 System Security

7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy as they are made known to the Contractor by the Authorized Recipient.

a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.

7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

a. CHRI shall be stored in a physically secure location.

b. The Authorized Recipient shall ensure that a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient must be identified by an ORI or state assigned identifier, and each Contractor or sub-Contractor must be uniquely identified.

8.0 Security violations

8.01 Duties of the Authorized Recipient and Contractor

a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.

b. Pending investigation, the Contractor shall immediately suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

c. The Contractor shall immediately notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

d. The Authorized Recipient shall immediately notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the

Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

8.02 Termination of the contract by the Authorized Recipient for security violations

a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.

b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.

c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.

8.03 Suspension or termination of the exchange of CHRI for security violations

a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 C.F.R. §906.2(d).

b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United

States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be immediately deleted or returned as specified by the Authorized Recipient.

8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:

a. The termination of a contract for security violations.

b. Security violations involving the unauthorized access to CHRI.

c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 Miscellaneous provisions

9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), CJIS Systems Agency, and the FBI.

9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) the CJIS Security Policy.

9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.[10]

9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.

9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.

9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer,

[10] Such conditions could include additional audits, fees, or security requirements.

Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer

1000 Custer Hollow Road

Module C 3

Clarksburg, WV 26306

Dated: _____ _____

Donna M. Uzzell

Compact Council Chairman

BILLING CODE 4410-02P

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Notice of approved methods of positive identification for noncriminal justice purposes.

Authority: 42 U.S.C., 14616.

SUMMARY: At its May 2004 meeting the Compact Council, established by the National Crime Prevention and Privacy Compact (Compact), approved two methods for determining positive identification [defined in Article I (20) of the Compact] for noncriminal justice purposes. For future updates to the Compact Council's list of approved methods of positive identification for noncriminal justice purposes, interested parties should contact the FBI's Compact Council Office.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Comments concerning this notice may be mailed to the FBI CJIS Division, Attn: FBI Compact Officer, Module C-3, 1000 Custer Hollow Road, Clarksburg, WV 26306, or comments may be submitted by facsimile to the

FBI Compact Officer at (304) 625-5388. Comments may also be sent by electronic mail (e-mail) to: tcommodo@leo.gov. Please submit e-mail comments in a Corel Word Perfect file, Microsoft Word file, or ASCII file format along with your name, agency name, and contact information. Please identify all comments in electronic form as "Comments to Definition of Positive Identification".

SUPPLEMENTARY INFORMATION: Pursuant to title 42, United States Code, § 14616, Article VI(e), the Compact Council is publishing this notice of two approved methods for determining positive identification for noncriminal justice purposes. By way of background, Article I (20) of the Compact defines positive identification as:

> "The term 'positive identification' means a determination, based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subject's names or other nonunique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification."

Due to innovative noncriminal justice initiatives in both state and federal communities, the Compact Council has received a myriad of inquiries regarding the Compact Council's interpretation of this definition. In order to clarify the Compact's definition of positive identification, ~~and under the authority of Article XI(a)(1)(A),~~ the Compact Council has approved two methods for determining positive identification for exchanging criminal history record information (CHRI) for noncriminal justice purposes.

In the criminal justice community, ten-rolled fingerprints has been the method to determine positive identification for over 80 years. The use of ten-rolled fingerprints has also served as the standard business practice in the noncriminal justice community. As a result of this long standing practice and reliability of using ten-rolled fingerprints to determine positive identification, the Compact Council formally accepted ten-rolled fingerprints as one method of positive identification for exchanging CHRI for noncriminal justice purposes.

In support of the recent National Fingerprint-based Applicant Check Study (N-FACS) conducted by the FBI's Criminal Justice Information Services (CJIS) Division,

the Compact Council examined the N-FACS results regarding the reliability of using ten-flat fingerprints for determining positive identification. After close examination of various N-FACS pilot program findings, the Compact Council formally accepted ten-flat fingerprints as another method for determining positive identification for noncriminal justice purposes. ~~Each authorized state or federal agency should coordinate the submission of ten-flat fingerprints with the FBI's CJIS Division.~~

Further, the definition in Article I (20) of the Compact refers to a "comparison of fingerprints" without specifying the number of fingerprint images. Accordingly, the Compact Council has determined that the definition is flexible enough to accommodate any future position the Compact Council may favor concerning the use of less than ten-rolled or ten-flat fingerprints when acceptable reliability is sufficiently documented. ~~The Compact Council recommends that f~~**F**uture alternatives for determining positive identification **must** be coordinated with the FBI's CJIS Division~~,~~ and ~~that~~ the scientific reliability ~~may~~ **should** not significantly deviate from the reliability of ten-rolled fingerprints, ten-flat fingerprints, and other **Compact Council** accepted methods for positive identification for noncriminal justice

purposes**; nor shall it degrade the search accuracy and/or computing capacity of the FBI's CJIS Division's Integrated Automated Fingerprint Identification System (IAFIS).**

FOR FURTHER INFORMATION CONTACT: Mr. Todd C. Commodore, 304-625-2803.

Dated: _____ _____

Donna Uzzell
Chairman
Compact Council

Department of State, Bureau of Consular Affairs Two-Print Pilot

Criminal Justice Information Services Division
Federal Bureau of Investigation

Common Objective

Prevent Terrorism
and
Promote the Nation's Security

National Crime Prevention and Privacy Compact Definition

Positive Identification: A determination, based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System.

Definition Clarification

After close examination of various National Fingerprint-based Applicant Check Study (N-FACS) pilot program findings, the Compact Council formally accepted ten-flat fingerprints as another method for determining positive identification for noncriminal justice purposes.

Department of State, Bureau of Consular Affairs Pilot Projects

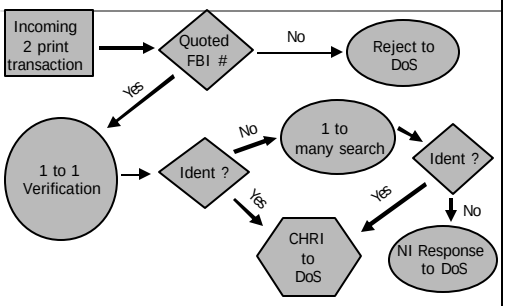
- After CLASS Hit
  - Ciudad Juarez, Mexico
  - Mexico City, Mexico
  - Guadalajara, Mexico
  - Monterrey, Mexico
- After IDENT Hit
  - San Salvador

Location	Prints	Date	Total Processed
Mexico City, Mexico	10 flats and rolled **electronic**	May 2003	16 months= 5,700
Ciudad Juarez, Mexico	10 flats and rolled **electronic**	Nov 2003	11 months= 1,600
Guadalajara, Mexico	10 flats Single digit Scanner	April 2004	5 months= 1,100
Monterrey, Mexico	Slap Device	Sept 28, 2004	1 month = 127

San Salvador Pilot

- 2-print Visa applicant search against the IDENT U.S. VISIT System at the San Salvador Consulate Office
- DOS, Bureau of Consular Affairs, will submit the two prints electronically to the to CJIS Division with
  - Quoted FBI Number
  - 2 flat index fingerprint images
  - Limited biographic information

IAFIS Process Flow



Study Deliverables

Six month study will determine:

- Best business process to perform 2 print verifications
- Processing resources required for 2 print identifications
- Success rates of comparisons, identifications, and verifications
- Whether the verification process serves the needs of both the FBI and the State Department

With State Department concurrence, the final study report will be presented to the Compact Council

Questions?

Tracy Pacoe
FBI, CJIS Division
304-625-4317

PROTECT ACT PILOT PROGRAM

Status Report

What is the PROTECT Act?

- In April 2003, the President signed into law the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act.
- The Act required the Attorney General to establish a pilot program for volunteer groups to obtain national and state fingerprint-based criminal history background checks.
  - National Mentoring Partnership
  - Boy & Girls Clubs of America
  - National Council of Youth Sports
- The pilot program began on July 29, 2003 and will end January 31, 2005 (18 months)

11/01/2004

What is the purpose of the pilot program?

- The purpose of the pilot program is to evaluate models for performing criminal background checks on individuals who work with children, the elderly and the disabled.

11/01/2004

Who is participating in the pilot program?

- Participating States
  - Montana
  - Tennessee
  - Virginia
  - Florida
- Volunteer Organizations
  - National Mentoring Partnership
  - Boys & Girls Clubs of America
  - National Council of Youth Sports

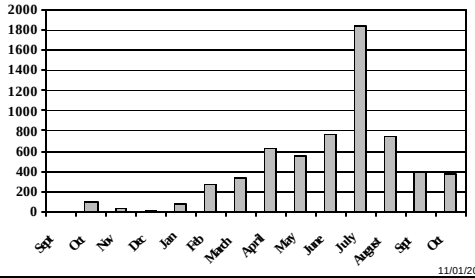
11/01/2004

Fitness Determinations

- The National Center for Missing and Exploited Children makes the determination whether an individual has a criminal history record that renders him or her unfit to provide care to children based on the following criteria:
  - All felonies.
  - Any lesser crime involving force or threat of force against a person.
  - Any lesser crime in which sexual relations is an element, including "victimless" crimes.
  - Any lesser crime involving controlled substances (not paraphernalia or alcohol).
  - Any lesser crime involving cruelty to animals.

11/01/2004

Total Submissions Received



11/01/2004

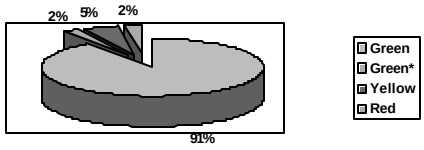
Status of Background Checks*

- Total submissions received – 6,225
- Total number of rejections – 1,110
- Reject rate – 18 percent
- Total submissions processed – 5,115
- Total number of identifications – 510
- Identification rate – 10 percent
- Appeals/Requests for criminal history records received – 49
  - 16 records were updated

* As of 11/01/2004

11/01/2004

Results of Fitness Determinations



* Green with record

11/01/2004

Accomplishments

- The FBI CJIS Division has test several new technical and operational processes
  - Manual In – Electronic Out
  - Paper Check Conversion
  - Electronic Submission of fingerprints via LEO
  - Record Challenge Process

11/01/2004

Other Issues

- Survey of volunteer organizations
- Ad Hoc studies
- Proposed extension of the pilot program

11/01/2004

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

28 CFR Part 904

[NCPPC 108]

Criminal History Record Screening for Authorized Noncriminal Justice Purposes

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Proposed rule, with request for comments.

SUMMARY: The Compact Council, established pursuant to the National Crime Prevention and Privacy Compact (Compact), is publishing a rule to establish criminal history record screening standards for criminal history record information received from the Interstate Identification Index (III) for authorized noncriminal justice purposes.

DATE: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Send all written comments concerning this proposed rule to the Compact Council Office, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306; Attention: Todd C. Commodore. Comments may also be submitted by fax at (304)625-5388 ~~or by electronic mail at tcommodo@leo.gov~~. To ensure proper handling, please reference "Record Screening Procedures Docket No. 108" on your correspondence. You may view an electronic version of this proposed rule at www.regulations.gov. You may also comment via electronic mail at tcommodo@leo.gov or by using the www.regulations.gov comment form for this regulation. When submitting comments electronically you must include NCPPC Docket No. 108 in the subject box.

FOR FURTHER INFORMATION CONTACT: Ms. Donna M. Uzzell, Compact Council

Chairman, Florida Department of Law Enforcement, P. O. Box 1489, Tallahassee, FL 32302, telephone number (850) 410-7100.

SUPPLEMENTARY INFORMATION:

The National Crime Prevention and Privacy Compact, 42 U.S.C. 14611-16, ~~(the Compact)~~ establishes uniform standards and processes for the interstate and federal-state exchange of criminal history records for noncriminal justice purposes. The Compact was approved by the Congress on October 9, 1998, (Pub. L. 105-251) and became effective on April 28, 1999, when ratified by the second state.

~~Prior to the enactment of the Compact and the National Fingerprint File Program, the FBI provided its criminal history records in response to authorized noncriminal justice requests. States that used the III System for noncriminal justice and criminal justice purposes were subject to the rules established by the Director of the FBI regarding that use. [See 28 CFR Part 0.85(j)].~~ Article VI of the Compact establishes a Compact Council "which shall have the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes, not to conflict with FBI administration of the III system for criminal justice purposes". The Council ~~finds~~ is proposing this rule ~~to be consistent with the intent~~ under the authority of Compact Article VI.

~~**Background:**~~

The Compact requires that each Party State appoint a Compact officer to regulate the in-state use of records received by means of the III system from the FBI or from other Party States. Since January 2003, Nonparty States may sign a memorandum of understanding (MOU) with the

Compact Council voluntarily binding the Signatory Nonparty States to the Council's rules, procedures, and standards for the noncriminal justice use of the III System. The MOUs between Nonparty States and the Compact Council are one mechanism to ensure system policy compliance until the states become Compact signatories. In order to implement Article IV(c)~~(3)~~, which provides inter alia that records obtained under the Compact by the requesting jurisdiction may only be used for the purpose requested and that the receiving jurisdiction must delete entries that may not legally be used for a particular noncriminal justice purpose, the Compact Council is ~~establishing~~ proposing this rule to ensure that only legally authorized records are used for particular noncriminal justice purposes. This proposed rule will also facilitate national uniformity in criminal history record screening and editing practices applicable to information received via the III System for noncriminal justice purposes.

Administrative Procedures and Executive Orders

Administrative Procedures Act

This rule is published by the Compact Council as authorized by the National Crime Prevention and Privacy Compact (Compact), an interstate/federal compact which was approved and enacted into law by Congress pursuant to Pub. L. 105-251. The Compact Council is composed of 15 members (with 11 state and local governmental representatives)~~, and is authorized by the Compact to promulgate rules and procedures for the effective and proper use of the Interstate Identification Index (III) System for noncriminal justice purposes~~. The Compact specifically provides that the Council shall prescribe rules and procedures for the

effective and proper use of the III System for noncriminal justice purposes, and mandates that such rules, procedures, or standards established by the Council shall be published in the Federal Register. *See* 42 U.S.C. 14616, Articles II(4), VI(a)(1), and VI(e). This publication complies with those requirements.

Executive Order 12866

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 12866 is not applicable.

Executive Order 13132

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 13132 is not applicable. Nonetheless, this Rule fully complies with the intent that the national government should be deferential to the States when taking action that affects the policymaking discretion of the States.

Executive Order 12988

The Compact Council is not an executive agency or independent establishment as defined in 5 U.S.C. 105; accordingly, Executive Order 12988 is not applicable.

Unfunded Mandates Reform Act

Approximately 75 percent of the Compact Council members are representatives of state and local governments; accordingly, rules prescribed by the Compact Council are not Federal mandates. Accordingly, no actions are deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

The Small Business Regulatory Enforcement Fairness Act (Title 5, U.S.C. 801-804) is not applicable to the Council’s rule because the Compact Council is not a "Federal agency" as defined by 5 U.S.C. 804(1). Likewise, the reporting requirement of the Congressional Review Act (Subtitle E of the Small Business Regulatory Enforcement Fairness Act)

does not apply. *See* 5 U.S.C. 804.

List of Subjects in 28 CFR Part 904

Crime, Health, Privacy

Accordingly, title 28 of the Code of Federal Regulations, Chapter IX is amended by adding part 904 to read as follows:

PART 904--STATE CRIMINAL HISTORY RECORD SCREENING STANDARDS

Sec.
904.1 Purpose and authority.
904.2 Interpretation of the criminal history record screening requirement.
904.3 State criminal history record screening standards.

Authority: 42 U.S.C. 14616

Sec. 904.1 Purpose and authority.

Pursuant to the National Crime Prevention and Privacy Compact (Compact), title 42, U.S.C., chapter 140, subchapter II, section 14616, Article IV (c)~~(3)~~, the Compact Council hereby establishes record screening standards for criminal history record information received by means of the III System for noncriminal justice purposes.

Sec. 904.2 Interpretation of the criminal history record screening requirement.

~~The Compact Council established pursuant to Article VI has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.~~ Compact Article IV(c)~~,~~ provides that "Any record obtained under this Compact may be used only for the official purposes for which the record was requested." Further, Article III(b)(1)(C)~~, of the Compact~~ requires that each Party State appoint a Compact officer who shall "regulate the in-~~s~~State use of records received by means of the III System from the FBI or from other

Party States." To ensure compliance with this requirement ~~in compact states~~, Compact Officers receiving records from the FBI or other Party States are specifically required to "ensure that record entries that may not legally be used for a particular noncriminal justice purpose are deleted from the response and, if no information authorized for release remains, an appropriate 'no record' response is communicated to the requesting official."~~ The Compact Council, pursuant to its authority under Article VI, is issuing this rule to facilitate national uniformity in criminal history record screening and editing practices applicable to information received via the III system for noncriminal justice purposes.~~ Compact Article IV(c)(3).

Sec. 904.3 State criminal history record screening standards

~~The following record screening standards relate to criminal history record information received for noncriminal justice purposes as a result of a national search utilizing the III System.~~ In performing their obligations under Sec. 904.2, Compact Officers shall ensure that the record screening procedures as set forth below are followed.

~~(a) The state receiving the record will screen the record to determine what information may legally be disseminated for the authorized purpose for which the record was requested. Screening will be conducted pursuant to the receiving state's applicable statute, executive order or state attorney general formal determination.~~

(a~~b~~) The State Criminal History Record Repository or an authorized agency in the receiving state will complete the record screening required under Sec. 904.2 for all noncriminal justice purposes.

(bc) ~~The state receiving the record may, at its discretion, decide whether that state's statute, executive order, or state attorney general formal determination provides specific record screening guidance concerning records received by means of the III System from the FBI or other states. If such guidance exists, the record screening and dissemination shall be based on the statute, executive order, or state attorney general formal determination.~~ Authorized officials performing record screening under Sec. 904.3(a) shall screen the record to determine what information may legally be disseminated for the authorized purpose for which the record was requested. Such record screening will be conducted pursuant to the receiving state's applicable statute, executive order, regulation, formal determination or directive of the state attorney general, or other applicable legal authority.

(cd) If the state receiving the record ~~receiving state's laws are silent~~ has no law, regulation, executive order, state attorney general directive, or other legal authority providing guidance on the screening of criminal history record information ~~from~~ received from the FBI or another state as a result of a national search ~~and absent an executive order or formal determination by the state attorney general~~, then the record screening under Sec. 904.3(a) shall be performed ~~is to be screened~~ in the same manner in which the state screens its own records for noncriminal justice purposes.

Dated: _____ _____

Donna M. Uzzell

Compact Council Chairman

BILLING CODE: 4410-02P

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

28 CFR Part 905

[NCPPC 109]

Qualification Requirements for Participation in the National Fingerprint File Program

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Proposed rule.

SUMMARY: The Compact Council (Council), established pursuant to the National Crime Prevention and Privacy Compact (Compact) Act of 1998, is publishing a proposed rule requiring a Compact Party to meet minimum qualification standards while participating in the National Fingerprint File (NFF) Program.

DATE: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Send all written comments concerning this proposed rule to the Compact Council Office, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306; Attention: Todd C. Commodore. Comments may also be submitted by fax at (304) 625-5388. ~~or by electronic mail at tcommodo@leo.gov~~. To ensure proper handling, please reference "NFF Program Qualification Requirements Docket No. 109" on your correspondence. You may view an electronic version of this proposed rule at www.regulations.gov. You may also comment via electronic mail at tcommodo@leo.gov or by using the www.regulations.gov comment form for this regulation. When submitting comments electronically you must include NCPPC Docket No. 109 in the subject box.

FOR FURTHER INFORMATION CONTACT: Ms. Donna M. Uzzell, Compact Council Chairman, Florida Department of Law Enforcement, P. O. Box 1489, Tallahassee, FL 32302, telephone number (850) 410-7100.

SUPPLEMENTARY INFORMATION:

This proposed rule requires all Compact Parties to comply with minimum qualification standards while participating in the NFF Program. The standards entitled "National Fingerprint File Qualification Requirements" are published in the Notices section of today's Federal Register; hereafter, interested parties should acquire a copy of the most current NFF Qualification Requirements by contacting the Compact Council Office at the address shown above.

Background

Compact Article VI establishes a Council which has "the authority to promulgate rules and procedures governing the use of the ~~FBI's~~ Interstate Identification Index (III) System for noncriminal justice purposes, not to conflict with the FBI administration of the III System for criminal justice purposes." The Council believes the promulgation of this rule and its accompanying notice will clarify for current and future NFF Program participants the requirements by which a participant's NFF performance will be measured. The notice related to this proposed rule contains two sets of Qualification Requirements - one applicable to State NFF participants and an analogous set for the FBI's NFF participation. The following paragraphs provide justification for both State and FBI participation in the NFF.

Party State NFF Participation

Compact Article III outlines the responsibilities of the Compact Parties. Article III(b)(3) provides that each Compact Party State shall participate in the NFF. See 42 U.S.C. 14616, Article III. The Compact does not set out a time line for NFF participation; to date, six Compact Party States participate in the NFF, while an additional ~~eight~~nine are in various stages of preparation to join the NFF Program. The FBI Criminal Justice Information Services (CJIS) Division's staff provides training and guidance to criminal history record repository staff as the State prepares for NFF participation.

The CJIS Audit staff will measure a State's performance in the NFF Program using audit criteria that align with the State NFF Qualification Requirements. The Council will publish a proposed rule establishing sanctions for noncompliance with its rules, procedures, and standards for the noncriminal justice use of the III System. The sanctions process outlined therein will be used by the Council to address noncompliance findings related to the noncriminal justice use of III, while noncompliance findings related to the criminal justice use of III will continue to be handled by the CJIS Advisory Policy Board (APB).

FBI NFF Participation

The FBI CJIS Division ~~(previously the Identification Division)~~ has maintained the NFF since its inception in 1991 as a pilot project. The CJIS Division remains an integral part of the NFF Program which, when fully implemented, will result in a national decentralized criminal history record system. Article II of the Compact requires the FBI to, among other things, permit use of the National Identification Index and the NFF by each Party State. Article II also

establishes an obligation for all Compact Parties to adhere to the Compact and the Compact Council's related rules, procedures, and standards.

Compact Article III requires the FBI Director-appointed Compact Officer to ensure the Department of Justice and other agencies and organizations that submit criminal history search requests to the FBI comply with the provisions of the Compact and with the Council's rules, procedures, and standards governing the use the III System for noncriminal justice purposes. Audit reports of the FBI's criminal history record repository will be provided to the Council, which will use the results to ensure CJIS Division compliance with the FBI NFF Qualification Requirements. (The FBI and its CJIS APB maintain purview over the criminal justice use of the III system. The APB has endorsed the referenced NFF Qualification Requirements and will be consulted in any future revisions.)

Administrative Procedures and Executive Orders

Administrative Procedures Act

The Compact Council, composed of 15 members including 11 state and local governmental representatives, is authorized to promulgate rules, procedures, and standards for the effective and proper use of the III System for noncriminal justice purposes. The Compact Council is publishing this rule in compliance with the mandate that rules, procedures, or standards established by the Council be published in the Federal Register. See 42 U.S.C. 14616, Articles II(4), VI(a)(1), and VI(e). This publication complies with those requirements.

Executive Order 12866

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 12866 is not applicable.

Executive Order 13132

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 13132 is not applicable. Nonetheless, this rule fully complies with the intent that the national government should be deferential to the States when taking action that affects the policymaking discretion of the States.

Executive Order 12988

The Compact Council is not an executive agency or independent establishment as defined in 5 U.S.C. 105; accordingly, Executive Order 12988 is not applicable.

Unfunded Mandates Reform Act

Approximately 75 percent of the Compact Council members are representatives of state and local governments; accordingly, rules prescribed by the Compact Council are not Federal mandates. Accordingly, no actions are deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

The Small Business Regulatory Enforcement Fairness Act (~~Title 5,~~ U.S.C. 801-804) is not applicable to the Council's rule because the Compact Council is not a "Federal agency" as defined by 5 U.S.C. 804(1). Likewise, the reporting requirement of the Congressional Review Act (Subtitle E of the Small Business Regulatory Enforcement Fairness Act) does not apply. See 5 U.S.C. 804.

List of Subjects in 28 CFR Part 905

Crime, Privacy, Information, Safety

Accordingly, ~~T~~title 28 of the Code of Federal Regulations is amended by adding Part 905 to read as follows:

Part 905--NATIONAL FINGERPRINT FILE (NFF) PROGRAM QUALIFICATION REQUIREMENTS

Sec.
905.1 Purpose and authority.
905.2 Participation in the NFF Program

Authority: 42 U.S.C. 14616.

§905.1 Purpose and authority.

The purpose of this part 905 is to require each NFF participant to meet the standards set forth in the NFF Qualification Requirements as established by the Compact Council (Council). The Council is established pursuant to the National Crime Prevention and Privacy Compact Act (Compact), ~~T~~title 42, U.S.C., ~~Chapter 140, Subchapter II, Section~~ § 14616.

§ 905.2 Participation in the NFF

Each NFF Program participant shall meet the standards set forth in the NFF Qualification Requirements as established by the Council and endorsed by the FBI's Criminal Justice Information Services Advisory Policy Board. Each participant's performance will be audited and measured by criteria designed to assess compliance with those requirements.

Dated: _____ _____

Donna M. Uzzell,

Compact Council Chairman

Joint Task Force on Rap Sheet Standardization

Compact Council
November 2004

Objectives of the JTF

- Develop a standardized criminal history transmission format
- Develop a standardized presentation format
- Develop a concept of operations which combines criminal histories from multiple sources into a single criminal history

Current Participants (version 2.2x)

- Maine
  - Intrastate September 2002
- Wisconsin
  - Intrastate August 2003
  - NLETS October 2003
- Kentucky
  - Included JTF specification with new criminal history system October 2003
- FBI
  - June 2004

Volume of Responses

- June 2004 585,657
- July 2004 694,595
- August 2004 729,349

Stylesheet

- XML transmission format vs Stylesheet
  - Stylesheet is presentation (and transformation)
  - One transmission format
  - NLETS provides default stylesheet
  - Customized stylesheet

Stylesheet Changes June 2004

- Typical rap sheet size
- Displayed agency name
- Did not impact informational content
- Reduction from 1029 to 612 lines (40%)
- Specific changes
  - Eliminated white space
  - Eliminated separator lines between cycle components
  - Removed text tags where there is no data (weight not provided)
  - Removed sections where no data provided

Global Justice Information Sharing Initiative

- Global operates under the auspices of the Office of Justice Programs (OJP), U.S. Department of Justice
- Global advises the federal government, specifically through the Assistant Attorney General, OJP, and the U.S. Attorney General, on justice information sharing and integration initiatives

Global Justice XML Data Model (GJXDM)

- Built on work of standardized rap sheet and others
- Intended to be a data reference model for the exchange of information within the justice and public safety communities.
- GJXDM and its associated GJXDD are intended to be used in the development and implementation of electronic information exchanges among justice, public safety and homeland security agencies.

Standardized Rap Sheet Version 3.0

- Based on GJXDM 3.0.2
- Informational content unchanged
- Stylesheet changes implemented in current version also included in 3.0
- Available at NLETS.ORG – target date November 16, 2004

Future Issues

- Merge rap sheets
- Summary section
- Index responses (multi-hit)
- No record responses

NLETS XML Implementers Conference

- Assist XML developers with implementing standardized rap sheet
- One day session on rap sheet
- January 12, 2005
- Phoenix, AZ
- Details to NLETS representatives

Submitting Name Checks via LEO

Presented by
FBI, Criminal Justice Information Services Division
Identification & Investigative Services Section

Background

- Why is the Name Check Service offered?
  - Civil submissions rejected twice due to poor image quality.
  - Alternative for individuals that cannot obtain a fingerprint check due to low quality of fingerprints (maybe due to age, occupation, heredity, etc.)
  - Agencies that have authority to submit fingerprints for non-criminal justice purposes.

Background

- The CJIS legacy system, Identification Automated System (IDAS), design enabled the contributor to safely assume a name check had been performed prior to rejection of a submission.
  - "A Name Check was performed with negative results." (Form1-17a)
- Since the implementation of IAFIS in July of 1999, this assumption can no longer be made. The name search may or may not have occurred based on the point of processing where the submission was rejected.

Name Check Process Established

- The manual name check process was established in September 5, 2001, for civil submissions rejected twice due to image quality.
- Image quality rejects: L0008, L0116, L0117, L0118.

Name Check Request

- Information required by the requesting agency via facsimile or mail :
  - Transaction Control Number (TCN) of rejected fingerprint submissions
  - Originating Agency Identifier (ORI)
  - Point of Contact information – name, phone number and facsimile number
  - Agency address
  - Required fields include name, DOB
    - Sex and Race are not required but Sex is preferable

FBI Responsibility

- FBI personnel confirms requested subject was rejected twice for image quality
- Return request to agency if all required information is not provided, or unable to verify that submissions have been rejected twice
- Notify agency by response/letter if negative search results are found

"Automating" the Name Check Process

- Recommended automation of the Name Check process
  - By modifying the L0008 reject message.
- L0008 error message was modified to identify if name search candidates were found when the III portion of the IAFIS search was performed.
  - If candidates are found, the message states: "The Quality of characteristics is too low to be used. However, possible candidates were found. Please submit a new set of fingerprints for comparison to the candidate (s)"
  - If no candidate was found, the message states: "The Quality of characteristics is too low to be used."

Enhancements to Program

- **Ability to submit request via LEO now available!!**
- Response may be returned via email (must be LEO)
- Benefits
  - Paperless
  - More convenient

Name Checks via LEO

- Form is located under LEOSIG
  - PUBLIC SIG
  - CJIS
  - PROGRAMS
  - III
  - On-Line Namesearch Form

Or at the following internet address:

- http://home.leo.gov/lesig/cjis/programs/iii/namesearch/Name_search_request.htm

Questions?

- For Further information contact the IISS Customer Service Area
  - Telephone (304)625-5590

  or
  - Email us at (NameCheck@LEO.gov or Liaison@LEO.gov)
- Need access to LEO? Contact Stacey Davis at (304) 625-2618